REMARKS/ARGUMENTS

The Office Action dated December 26, 2007, has been reviewed and the following remarks are responsive thereto. Claims 48, 59, 75, 76, 80, 83-85, 92 and 99 have been amended. Claim 102 has been cancelled without prejudice or disclaimer. Claims 103-107 have been added. No new matter has been added. Claims 48-85, 92, 95-101 and 103-107 remain pending upon entry of the present amendment.

Claim Rejections

Claims 48-50, 54-71, 77, 80-85, 92 and 95-101 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Theimer *et al.* (U.S. Patent No. 5,649,099, "Theimer") in view of Guski *et al.* (U.S. Patent No. 6,711,679). Claims 51 and 82 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Theimer in view of Guski and Shin *et al.* (U.S. Patent No. 5,987,134, "Shin"). Claims 52, 53, 78, 79 and 102 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Theimer in view of Guski and Scott *et al.* (U.S. Patent No. 6,484,260, "Scott"0. Claims 72-76 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Theimer in view of Guski and Wang (U.S. Patent No. 6,175,922). Applicants respectfully traverse these rejections.

Amended independent claims 48 and 92 recite, *inter alia*, a first electronic key device authorized to unlock an electronic lock device and configured to generate an electronic ticket for providing a second electronic key device authorization to unlock the electronic lock device. Claim 48 further recites that the electronic ticket includes a public key corresponding to the second key device, wherein the public key is configured to decrypt a code issued by the electronic lock device and encrypted by the second key device. For example, Theimer merely describes executing an access control program to determine whether or not to grant access. Abstract. There is no teaching or suggestion in Theimer of using a public key of a second key device to verify whether the second key device is authorized to unlock a lock device by decrypting a code issued by the lock device. Guski is similarly deficient. While Guski describes a server acting as a delegate for a client by using certification data structures that include certificates of the client and the server, Guski does not teach or suggest that the public key of the server (i.e., the alleged second key device) is configured to decrypt a code issued by a lock

device and encrypted by the server. Col. 7, ll. 20-65. None of the other cited references cure the deficiencies identified above. Accordingly, notwithstanding whether the references are properly combinable, the asserted combination would not have resulted in the features recited in claims 48 and 92. Claims 48 and 92 are thus allowable for at least these reasons.

Claims 59 and 99 recite, *inter alia*, a first key device receiving an electronic ticket transmitted from a second electronic key device authorized to unlock an electronic lock device, wherein the at least one received electronic ticket comprises a public key corresponding to the first key device, receiving a code issued by the electronic lock device, encrypting the code using a private key of the first electronic key device, and transmitting the encrypted code to the first electronic key device. The cited references fail to teach or suggest such features. As discussed above, Guski merely describes the use of certification data structures to allow a server to act as a client's delegate. Nonetheless, there is no teaching or suggestion in Guski of receiving a code issued by a lock device, encrypting the code and transmitting the encrypted code back to the lock device. None of the other references are able to cure these deficiencies of Guski. Accordingly, claims 59 and 99 are allowable for at least these reasons.

Claim 80 recites, *inter alia*, a lock device configured to receive an encrypted code corresponding to the issued code encrypted using a private key of the first electronic key device, determine a decrypted code by decrypting the encrypted code using the public key of the first electronic key device, and determine whether the decrypted code matches the issued code. Nowhere do any of the cited references teach or suggest such features. For example, neither Theiman nor Guski, either separately or in combination, teaches or suggests decrypting a code encrypted by a key device using a public key of the key device included in a ticket received from the key device. Guski merely describes extracting a public key from a certificate data structure (CDS) to verify that the server transmitting the CDS is authorized to act as a delegate based on whether the public key corresponds to the digital signature of the CDS. Guski makes no mention or suggestion of issuing a code to the key device, receiving an encrypted code, decrypting the code using a public key of the key device and determining whether the issued code and the decrypted code match, as recited in claim 80. The other cited references are similarly deficient. Accordingly, claim 80 is allowable for at least these reasons.

Claims 49-58, 60-79, 81-84, 95-98 and 100-101 are dependent on claims 48, 59, 80, 92 and 99, respectively, and are thus allowable for at least the same reasons as their base independent claim and further in view of the novel and non-obvious features recited therein. For example, claim 51 recites, *inter alia*, "wherein said electronic lock device stores public keys for a plurality of authorized key holders." Contrary to the assertions of the Office Action at p. 9, none of the cited references teach or suggest such a feature. For example, the Office Action relies on Shin to allegedly teach an electronic lock device storing a plurality of public keys for a plurality of authorized key holders. The Office Action's reliance is misplaced. Shin merely discloses an access ticket public key storing means that stores a modulus n used to generate challenging data C. Col. 11, ll. 1-9. Even assuming, without conceding, that modulus n constitutes a public key, Shin still does not teach or suggest that the access ticket public key storing means stores a *plurality* of public keys for a *plurality of authorized key holders*. Accordingly, claim 51 is allowable for this additional reason.

New Claims

Claims 103-107 have been added. While Applicants recognize that claims 103-105 have not been rejected, the following comments have been provided in the interest of expediting prosecution.

New independent claim 103 recites features similar to those discussed with respect to claim 80 and is thus allowable for at least the same reasons as claim 80. Claims 104 and 105 are dependent on claim 103 and is thus allowable for at least the same reasons as claim 103.

Claims 106 and 107 are dependent on claim 48 and are thus allowable for at least the same reasons as claim 48.

CONCLUSION

All rejections having been addressed, Applicant respectfully submits that the instant application is in condition for allowance, and respectfully solicits prompt notification of the same. The Office is hereby authorized to charge any fees due, including a three month extension of time fee, to Deposit Account 19-0733. If for any reason the Examiner believes the application is not in condition for allowance or there are any questions, the examiner is requested to contact the undersigned at (202) 824-3156.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: March 26, 2008

By: /Chunhsi Andy Mu/
Chunhsi Andy Mu, Reg. No. 58,216

1100 13th Street, N.W.
Washington, D.C. 20005
Tel: (202) 824-3000
Fax: (202) 824-3001